Analisis Overhead Penggunaan Digital Signature Pada Protokol MQTT

Husnul Hidayat[1], Parman Sukarno[2], Aulia Arif Wardana[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]husnulhidayat@students.telkomuniversity.ac.id, [2]psukarno@telkomuniversity.ac.id,
[3]auliawardana@telkomuniversity.ac.id

Abstract

This study proposes a digital signature scheme to secure messages sent by the publish/subscribe middleware Message Queue Telemetry Transport (MQTT) protocol. In which, it uses the Advanced Encryption System (AES) and Secure Hash Algorithm (SHA) with the end-to-end method and analyze the overhead of application of digital signature. Because, the disadvantage of MQTT is that there is no encryption process on the payload. In which, allows one to be able to find out the payload content that causes no privacy in the data. Data integrity is also a problem with MQTT. The purpose of this digital signature is to verify that the payload sent is a genuine one, which does not change during the transmission process, and the secrecy of the payload. After evaluating and testing the proposed system, the program can secure the MQTT payload. The addition of a security mechanism in MQTT such as the encryption process, decryption, verification results produces overhead in several aspects. The overhead used in this study is to measure the size of the payload, the time of sending messages, the process of the mechanism of digital signature security, memory consumption, and CPU usage. In an overhead analysis, overhead is carried out by examining various types of AES keys and multiple types of SHA. After examination, there is an increase in size for several aspects that have been mentioned because of the digital signature scheme.

Keywords: middleware, payload, AES, SHA, digital signature, overhead.